U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE

HEARING CHARTER

Cybersecurity: U.S. Vulnerability and Preparedness

Thursday, September 15, 2005
10:00 a.m. - Noon
2318 Rayburn House Office Building

1. Purpose

On Thursday, September 15, 2005, the House Science Committee will hold a hearing to examine the extent of U.S. vulnerability to cyber attacks on critical infrastructure such as utility systems, and what the federal government and private sector are doing, and should be doing, to prevent and prepare for such attacks. The hearing will also examine what duties should be given to the new Assistant Secretary for Cybersecurity and Telecommunications at the Department of Homeland Security.

2. Witnesses

Mr. Donald "Andy" Purdy is Acting Director of the National Cyber Security Division at the Department of Homeland Security (DHS). Prior to joining DHS, he served as senior advisor for Information Technology Security and Privacy to the President's Critical Infrastructure Protection Board.

Mr. John Leggate is the Chief Information Officer at BP Inc. (formerly known as British Petroleum). In addition, he is chairman of the Chief Executive Officers' Roundtable on Digital and Cyber Infrastructure Security at the industry organization Business Executives for National Security.

Mr. David Kepler is Corporate Vice President of Shared Services and Chief Information Officer of The Dow Chemical Company. In addition, he leads the Chemical Sector Cybersecurity Information Sharing Forum, an industry association.

Mr. Gerald Freese is the Director of Enterprise Information Security at American Electric Power, one of the largest electric utilities in the United States. He has also been active in the North American Electric Reliability Council-coordinated development of cyber security standards for the energy industry.

Mr. Andrew Geisse is the Chief Information Officer of SBC Services Inc. (formerly Southwestern Bell Corporation), the largest telecommunications carrier in the United States.

3. Overarching Questions

- How do critical infrastructure sectors depend on public and private information systems? What are the possible consequences for these sectors of disruption or attack on their information systems? What steps are being and should be taken to secure these systems?

- What are the most critical responsibilities of the Department of Homeland Security (DHS) in cybersecurity for critical infrastructure sectors, and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?

- In what areas are current cybersecurity technical solutions for critical infrastructure sectors inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How should federal agencies, such as DHS, the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), and the Defense Advanced Research Projects Agency (DARPA), and academic researchers work with industry to define priorities and support research in these areas?

4. Issues

Is the U.S. adequately protecting critical information systems and is the U.S. able to detect, respond to, and recover from a cyber attacks on critical infrastructure?

While industry and the federal government have increased their focus on cybersecurity in recent years, vulnerabilities remain, and many experts believe the U.S. needs to do more. An informal survey by a business group early this year found that, in the telecommunications, energy, chemical, and transportations industries, executives estimated that 20 to 35 percent of their revenue depends directly on the Internet. Yet despite the crucial role of information technology, the vulnerabilities in information technology systems are myriad. About 10 new entries are added each day to the National Vulnerability Database (maintained by the National Institute of Standards and Technology), which contains about 12,000 entries describing vulnerabilities in commonly used information technology products. (Statistics about attacks on critical infrastructure are hard to obtain because such attacks are often not reported.)

Is there a clear line of responsibility within the federal government to deal with cybersecurity?

When DHS was formed in 2002, cybersecurity responsibilities (other than research and development) were assigned to the Assistant Secretary for Infrastructure Protection. Ever since, industry representatives have repeatedly expressed concern that cybersecurity has been a distant second to physical security in DHS's critical infrastructure protection activities and that the lack of a high-level official dedicated to cybersecurity has meant that the Department has failed to devote attention and resources to cybersecurity. In May 2005, the Government Accountability Office (GAO) found that DHS was having trouble with a number of its cyber responsibilities, including developing national cyber threat and vulnerability assessments and government/industry contingency recovery plans for cybersecurity, establishing effective partnerships with stakeholders, and achieving two-way information sharing with these

stakeholders. (The summary of this report is included in Attachment A.) In response to Congressional and industry concerns, the Secretary of Homeland Security created in July the new position of Assistant Secretary for Cybersecurity and Telecommunications to bring a higher profile to this area and high level attention to these problems. The position has not yet been filled.

Are private companies doing enough to secure their information systems? To what extent are they coordinating with each other and the federal government on cybersecurity?

The record is mixed. For many companies, it can be difficult to quantify the risks associated with their dependence on information systems and hence difficult to justify investment in cybersecurity. In other cases, the relevant cybersecurity technologies may not be available. In many industries, companies have undertaken cybersecurity activities within industry organizations to set standards, share best practices, and work with information technology companies to improve the security of information systems and increase their cybersecurity options. (The companies testifying have generally been leaders in taking cybersecurity seriously.) In some cases, cybersecurity work has been hampered by the problems in the federal government described above. Industry groups have indicated that they do not yet trust the processes for sharing sensitive information related to their cybersecurity with the government and have not yet been convinced of the value of information and services DHS would provide in return.

What should the priorities be for federal cybersecurity research and development programs? Is funding for these programs adequate?

Recommended areas for federal cybersecurity research in general were outlined in the recent report[1] of the President's Information Technology Advisory Committee (PITAC) and include monitoring and detection technologies, software quality assurance processes, authentication techniques, mitigation and recovery technologies, and metrics, benchmarks, and best practices. The PITAC report recommended substantial increases in funding at the National Science Foundation (NSF), DHS, and the Defense Advanced Research Projects Agency (DARPA). (Currently, funding for cybersecurity research programs at NSF and the National Institute of Standards and Technology (NIST) is well below the levels authorized in the *Cyber Security Research and Development Act*.) The Cyber Security Industry Alliance, an association of cyber security software, hardware and services companies, the Internet Security Alliance, an association of information security users from sectors such as banking, insurance, and manufacturing, and the Information Technology Association of America, a trade association of the information technology industry, have all also publicly recommended increased federal funding for cybersecurity research and development.

[1] The President's Information Technology Advisory Committee released their report, *Cyber Security: A Crisis of Prioritization*, on March 18, 2005. It is available on line at http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

5. Brief Overview

- Critical infrastructure[2] sectors include electric power generation and transmission, oil and gas production and distribution, communications, chemicals, food production, banking and finance, transportation systems, and water processing systems. These sectors are increasingly dependent on information systems to administer business operations (such as billing and supply chain management) and to monitor and control physical operations (such as manufacturing processes and distribution systems).

- As reliance on information technology grows, the number of ways that critical infrastructure systems can be interfered with and the extent of disruption or damage that can be created via such interference is also growing. In addition, the potential impact of a combined physical and cyber attack on a critical facility—e.g. using disruption of information systems to interfere with response and recovery after an explosion—would be severe.

- Some cybersecurity products and techniques (such as firewalls, intrusion detection systems, and virus-protection checks) can be used to safeguard many types of standard information systems (e.g. protecting billing systems and customer databases). However, specialized information technology products are often used to manage and control critical infrastructure facilities. These process control systems often use customized or older hardware and software and have different performance requirements and hence may require specialized security solutions and strategies.

- In May 2005, GAO assessed the DHS role in cyber critical infrastructure protection and found that DHS was having trouble with a number of its cyber responsibilities, including developing national cyber threat and vulnerability assessments and government/industry contingency recovery plans for cybersecurity (including a plan for recovering key Internet functions), establishing effective partnerships with stakeholders, and achieving two-way information sharing with these stakeholders.

- In response to stakeholder and Congressional concerns that DHS needed to make information security, particularly information security for critical infrastructure sectors, a higher priority, the Secretary of Homeland Security announced in July 2005 that the Department would create a new position of Assistant Secretary for Cybersecurity and Telecommunications. This new position will have responsibility for identifying and assessing the vulnerability of critical telecommunications infrastructure and assets, providing timely and usable threat information, and leading the national response to cyber and telecommunications attacks.

- In information technology systems, new vulnerabilities and new threats emerge regularly and spread quickly. Cybersecurity research programs supported by the federal government and the private sector develop tools that provide security in the current environment, as well as produce the defenses against the next generation of cybersecurity risks. Following passage

[2] As defined in the USA PATRIOT Act (P.L. 107-56), critical infrastructure is "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters." This definition is used broadly throughout the federal government.

of the *Cyber Security Research and Development Act* in 2002, funding for National Science Foundation programs in this area has increased; however, at the same time the Defense Advanced Research Projects Agency funding for unclassified research in cybersecurity has dropped significantly. Other federal cybersecurity research and development programs exist, particularly at DHS and at the National Institute of Standards and Technology, but these are relatively small.

6. Background

Critical Infrastructure Sectors and Information Security

Critical infrastructure, as defined in the USA PATRIOT Act, is "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters." Examples of critical infrastructure include electric power generation and transmission, oil and gas production and distribution, communications, chemicals, agriculture and food processing, banking and finance, transportation systems, and water processing systems. Because of its vital role in the U.S. security, economy, and quality of life, the elements of the U.S. critical infrastructure are a potential target for terrorists, who could use physical or cyber attacks to interfere with, disrupt, damage, or destroy important facilities and capabilities.

Industry is increasingly dependent on information technology for both business operations and process controls, and many of these information systems directly use, or are accessible through, public systems (e.g., the Internet) and technologies (e.g., Wi-Fi and common operating systems). Yet the Internet was not designed with security in mind.

Control systems (systems that run manufacturing and distribution facilities) raise different security issues than do the business/administrative systems. It is harder to shut the control systems down to make changes in software or hardware because doing so means shutting down an industrial operation, such as chemical manufacturing or electricity generation. In addition, the control systems operate equipment that represents a major capital expense and that is replaced or upgraded less frequently than are business systems. As a result, security fixes to control systems often require retrofitting, rather than just waiting for equipment to be replaced. Finally, while business systems (for activities like billing) are relatively similar across industries, the control systems generally use specialized protocols and configurations specific to a particular industry. As a result, customized security solutions and strategies, including specialized testing, need to be developed.

Industry responses to cyber vulnerability has depended on: (1) the type of information systems used in the sector, (2) how clear the risks associated with cyber attacks are, (3) what the value and return on investment in cybersecurity would be, (4) the availability of relevant cybersecurity technologies, and (5) (sometimes) what governmental action has been taken or is perceived as having the potential to be taken. For example, the financial and banking industries were very aggressive in adopting information security technologies, due in part to the fact that technologies to protect information and communications (the primary need in this area) have been a focus of

cybersecurity development efforts for a long time because the extent of the vulnerability was very clear.

In other industries, there are a variety of cybersecurity-focused activities underway. In the electric power industry, the North American Electric Reliability Council (an industry coordination group) recently developed and adopted an interim cybersecurity standard that outlines minimum requirements needed to ensure the security of electronic exchange of information needed to support grid reliability and market operations; work on a permanent standard is underway. In addition, Congress has focused attention on cybersecurity as a key element of ensuring electric reliability and drinking water safety. The Environmental Protection Agency has worked with the industry on understanding how their water processing facilities depend on information systems and what risks that creates.

The chemical sector has developed a Chemical Sector Cybersecurity Program, which is building on existing cooperative industry groups to carry out cybersecurity-specific activities. A sector-wide cybersecurity strategy was organized in 2002, and activities currently underway include work on establishing management practices, guidelines, and standards, on information sharing, and on encouraging accelerated development of improved security technologies. In addition, the chemical sector companies involved with the program support legislation that will establish national security guidelines for chemical facilities, require companies to conduct site vulnerability assessments and implement security plans, and create strong enforcement authority to help ensure facilities and systems are secure.

In addition to specific cybersecurity activities, all critical infrastructure sectors have Information Sharing and Analysis Centers (ISACs), which provide a forum for companies to exchange, analyze and disseminate information about vulnerabilities, threats, and incidents in a trusted environment. (The establishment of ISACs was mainly a response to Presidential Decision Directive 63 (issued in 1998), which encouraged industry to form such groups. Each ISAC has a different structure and relationship with the government, depending on the specific industry's needs, history, and regulatory environment.) In general, discussion of cybersecurity issues are considered an important element of ISAC-based interactions, and cross-sector discussions of cybersecurity issues are coordinated by the information technology sector's ISAC.

Department of Homeland Security Cybersecurity Activities and Responsibilities

Cybersecurity activities at DHS are carried out in two directorates: the National Cyber Security Division (NCSD), located in the Information Analysis and Infrastructure Protection Directorate, is responsible for operational cybersecurity; and the Science and Technology Directorate is responsible for cybersecurity research and development programs.

Operational Cybersecurity at DHS

After the recently completed department-wide Second Stage Review, the Secretary of Homeland Security has proposed and begun to implement a number of organizational changes, including the creation of an Assistant Secretary for Cybersecurity and Telecommunications position. This office will be responsible for identifying and assessing the vulnerability of critical

telecommunications infrastructure and assets, providing timely and usable threat information, and leading the national response to cyber and telecommunications attacks. (To date, the NCSD has reported to the existing Assistant Secretary for Infrastructure Protection; going forward, the new Assistant Secretary will be parallel to this position.[3])

The responsibilities of the NCSD are defined by several documents, including the National Strategy to Secure Cyberspace, Homeland Security Presidential Directive 7 (HSPD-7) on Critical Infrastructure Identification, Prioritization, and Protection,[4] the Interim National Infrastructure Protection Plan, and the National Response Plan. In FY06, $73 million was requested for NCSD, a $6 million increase from the level appropriated for FY05. The NCSD's mission, as defined in HSPD-7, includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.[5] Currently, within these broad goals, three areas of particular concern and focus for NCSD in the area of critical infrastructure protection are (1) strategies to improve the resiliency of the Internet against disruption, (2) improving the security of control systems, and (3) improving software assurance (trying to move from patch management to systems that emphasize security as software is being developed).

One of the most important activities of NCSD is coordination with the private sector on efforts to reduce vulnerabilities and minimize the severity of cyber attacks. Information sharing is necessary to ensure awareness of vulnerabilities, and ways to mitigate vulnerabilities, awareness of threats and attack methods, and preparedness for response and recovery. Companies are expected to be a source of information about what problems they are experiencing and what solutions have been effective, while the government (primarily via DHS) is expected to be a source of information about threats. Both government and industry acknowledge that information sharing needs to be improved. Industry has been reluctant to share sensitive information incidents. In addition, it has been unclear whether DHS has developed the policies or attracted the expertise to ensure the confidentiality of sensitive information and to provide reliable analysis and feedback about threats and potential solutions.

A variety of activities are underway in the NCSD to carry out its mission. These include the U.S. Computer Emergency Readiness Team (US-CERT), which was established in 2003 as a partnership between DHS and the public and private sectors. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning

[3] The new Assistant Secretary for Cybersecurity and Telecommunications will be Presidentially appointed, but not Senate confirmed. The new position was announced on July 13, 2005, but as of the date of this hearing an appointment had not yet been made.

[4] Homeland Security Presidential Directive 7 (HSPD-7) on Critical Infrastructure Identification, Prioritization, and Protection is available on line at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[5] To meet its responsibilities from HSPD-7, as well as other national strategies and plans, NCSD has defined for itself six core goals: (1) establish a National Cyber Security Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents; (2) work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks; (3) promote a comprehensive national awareness program to empower American businesses, the general workforce, and the general population to secure their own parts of cyberspace; (4) foster adequate training and education programs to support the nation's cyber security needs; (5) coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and (6) build a world-class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

information, and coordinating incident response activities. Another key NCSD activity is organizing exercises to test preparedness and response plans for cyber attack. The next such exercise is scheduled for November 2005 and will include public and private sector participants, including companies from the energy, communications, and transportation sectors.

Cybersecurity Research and Development at DHS

Research and development related to cybersecurity are the responsibility of the DHS Science and Technology Directorate. In FY06, $16.7 million was requested for the cybersecurity programs in the Science and Technology Directorate, a $1.3 million decrease from the level appropriated for FY05. Specific programs focus on improving the security of Internet communication protocols and developing technologies to enhance the cybersecurity of critical infrastructure sectors, including of process control systems. Support and coordination is also provided for the collection of large-scale data sets about network behavior that researchers can use to better understand problems with networks and design potential solutions. Testbeds are also a critical element of DHS Science and Technology Directorate cybersecurity programs. They provide support for and participate in the NSF-funded Defense Technology Experimental Research (DETER) testbed (described below). They also work with the Department of Energy (at Sandia and Idaho National Laboratories) to support a control systems testbed, which is critical for design and verification of security technologies for control system applications. Since these systems often operate with real-time consequences and continuously or almost continuously, any security solution must be designed for the configuration in which the equipment and software is used and rigorously tested in realistic situations.

Cybersecurity at Other Government Agencies and Interagency Coordination

Operational Cybersecurity

Each critical infrastructure sector is associated with a lead government agency. For some sectors (e.g. chemicals, transportation systems, information technology and telecommunications), the lead agency is DHS, but for many other sectors, another agency is the lead (e.g. the Department of Energy for the electric power and oil and gas sectors, the Environmental Protection Agency for water treatment facilities, the Department of the Treasury for banking and finance, and the Department of Agriculture for the food sector). However, HSPD-7, the 2003 Presidential Directive that designated the lead agencies, also clearly articulated that DHS would continue to maintain an organization to serve as a focal point for the security of cyberspace. For example, DHS, the Department of Defense (DOD), and the Department of Justice co-chair the interagency National Cyber Response Coordination Group. In addition to coordinating with other agencies on the cybersecurity of critical infrastructure facilities, DHS also works with the Office of Management and Budget, which has significant responsibilities for the security of the federal government's information systems.

Cybersecurity Research and Development Programs

Significant cybersecurity research and development programs are underway in a variety of federal agencies, including the National Science Foundation (NSF), the National Institute of

Standards and Technology (NIST), and the Defense Advanced Research Projects Agency (DARPA). The programs at NSF and NIST were authorized by the *Cyber Security Research and Development Act* (P.L. 107-305).

At NSF, cybersecurity research is conducted under the auspices of the Cyber Trust program, which supports projects designed to make networked computer systems more predictable, more accountable, and less vulnerable to attack and abuse. This program is funded at $65 million in FY05, and the projects supported cover a wide variety of information security areas. Critical infrastructure applications are included; in August 2005, NSF provided funding to a new center at the University of Illinois to perform research to support the design, construction and validation of a secure cyberinfrastructure for the next-generation electric power grid. (Both the Department of Energy and DHS have pledged to collaborate with NSF to fund and manage this effort.) Another relevant project is the Cyber Defense Technology Experimental Research (DETER) testbed, which provides an experimental environment in which government, academic, and industry cyber-security researchers can safely analyze and measure attacks and develop attack mitigation and confinement strategies. (DHS also provides some funding for DETER.) These research and testbeds projects also have educational elements, as the laboratories supported by those funds become centers of expertise in information systems for critical infrastructure and train the personnel that critical infrastructure companies and information technology companies need to improve the security of critical infrastructure sector applications. In addition to its cybersecurity research programs, NSF also supports cybersecurity education activities, including scholarships and curriculum development (these programs received $16 million in FY05).

At NIST, cybersecurity activities are centered in the Computer Security Division, which was funded at $19 million in FY05. The division's activities include developing standards, metrics, tests, guidelines, and validation programs related to information security and studying and raising awareness of information technology risks, vulnerabilities, and protection requirements. NIST also has specific responsibilities under the *Federal Information Security Management Act of 2002* for developing standards for federal information systems security and supporting federal agencies' cybersecurity efforts. An example of a recent NIST cybersecurity project (supported by DHS) is the August 2005 launch of the National Vulnerability Database, which contains about 12,000 entries describing vulnerabilities in commonly-used information technology products. (About 10 new entries are added each day.) The database integrates all publicly available U.S. government vulnerability resources and is designed to provide references to industry resources.

A number of other agencies, mainly in the DOD, have cybersecurity research and development activities. The DOD activities focus mainly on specific information assurance requirements related to DOD's military and intelligence missions. The Department of Energy's programs are focused primarily on applications related to the energy and electric power sectors (as in the work on control systems testbeds at Department of Energy laboratories described above).

All of these programs are coordinated through the National Science and Technology Council's (NSTC's) Interagency Working Group on Critical Information Infrastructure Protection Research and Development. In response to recommendations from the President's Information Technology Advisory Committee, this interagency group has recently been reformulated to

report to both the NSTC Subcommittee on Infrastructure and its Subcommittee on Networking and Information Technology Research and Development. This group has recently begun work on defining top cybersecurity research and development needs and mapping those needs against current federal activities.

7. Witness Questions

Questions for Mr. Andy Purdy:

- How do critical infrastructure sectors depend on public and private information systems? What are the possible consequences for these sectors of disruption or attack on their information systems? What steps is DHS taking to help these sectors secure their systems?
- How does DHS work with the critical infrastructure sectors to gather and communicate information about threats, risks, and solutions related to cybersecurity?
- In what areas are current cybersecurity technical solutions for critical infrastructure applications inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How is DHS working with industry and academic researchers to define priorities for and support research in these areas? How does DHS coordinate these efforts within DHS and with other federal agencies, such as NSF, NIST, and DARPA?

Questions for Mr. John Leggate:

- How does the energy sector depend on public and private information systems? What are the possible consequences for the energy sector of disruption or attack on its information systems? What steps is BP taking to secure its systems?
- What are the most critical responsibilities of DHS in cybersecurity for the energy sector and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?
- In what areas are current cybersecurity technical solutions for the energy sector inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How should federal agencies, such as DHS, NSF, NIST, and DARPA, and academic researchers work with industry to define priorities for and support research in these areas?

Questions for Mr. David Kepler:

- How does the chemical sector depend on public and private information systems? What are the possible consequences for the chemical sector of disruption or attack on its information systems? What steps is Dow taking to secure its systems?
- What are the most critical responsibilities of DHS in cybersecurity for the chemical sector and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?
- In what areas are current cybersecurity technical solutions for the chemical sector inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How should federal agencies, such as DHS, NSF, NIST, and DARPA, and academic researchers work with industry to define priorities for and support research in these areas?

Questions for Mr. Gerald Freese:

- How does the electric power sector depend on public and private information systems? What are the possible consequences for the electric power sector of disruption or attack on its information systems? What steps is American Electric Power taking to secure its systems?
- What are the most critical responsibilities of DHS in cybersecurity for the electric power sector and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?
- In what areas are current cybersecurity technical solutions for the electric power sector inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How should federal agencies, such as DHS, NSF, NIST, and DARPA, and academic researchers work with industry to define priorities for and support research in these areas?

Questions for Mr. Andrew Geisse:

- How does the communications sector depend on public and private information systems? What are the possible consequences for the communications sector of disruption or attack on its information systems? What steps is SBC taking to secure its systems?
- What are the most critical responsibilities of DHS in cybersecurity for the communications sector and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?
- In what areas are current cybersecurity technical solutions for the communications sector inadequate? Where is further research needed to mitigate existing and emerging threats and vulnerabilities? How should federal agencies, such as DHS, NSF, NIST, and DARPA, and academic researchers work with industry to define priorities for and support research in these areas?

Attachment A

Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities

Government Accountability Office Report GAO-05-434
http://www.gao.gov/new.items/d05434.pdf

Excerpt: Results in Brief

As the focal point for critical infrastructure protection, DHS has many cybersecurity-related roles and responsibilities that are called for in law and policy. These responsibilities include developing plans, building partnerships, and improving information sharing, as well as implementing activities related to the five priorities in the national cyberspace strategy: (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. To fulfill its cybersecurity role, in June 2003, DHS established the National Cyber Security Division to serve as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts.

While DHS has initiated multiple efforts, it has not fully addressed any of the 13 key cybersecurity-related responsibilities that we identified in federal law and policy, and it has much work ahead in order to be able to fully address them. For example, DHS (1) has recently issued the Interim National Infrastructure Protection Plan, which includes cybersecurity elements; (2) operates the United States Computer Emergency Readiness Team to address the need for a national analysis and warning capability; and (3) has established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed national threat and vulnerability assessments or developed and exercised government and government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. Further, DHS continues to have difficulties in developing partnerships—as called for in federal policy—with other federal agencies, state and local governments, and the private sector.

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. Key challenges include achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal agencies, state and local governments, and the private sector); achieving two-way information sharing with these stakeholders; and demonstrating the value DHS can provide. In its strategic plan for cybersecurity, DHS has identified steps that can begin to address these challenges. However, until it effectively confronts and resolves these underlying challenges, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our nation's critical infrastructures, and our nation will lack the strong cybersecurity focal point envisioned in federal law and policy.

We are making recommendations to the Secretary of Homeland Security to strengthen the department's ability to implement key cybersecurity responsibilities by completing critical activities and resolving underlying challenges.

DHS provided written comments on a draft of this report (see app. III). In brief, DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remains to be done. In addition, DHS concurred with our recommendation to engage stakeholders in prioritizing its key cybersecurity responsibilities. However, DHS did not concur with our recommendations to identify and prioritize initiatives to address the challenges it faces, or to establish performance metrics and milestones for these initiatives. Specifically, DHS reported that its strategic plan for cybersecurity already provides a prioritized list, performance measures, and milestones to guide and track its activities. The department sought additional clarification of these recommendations. While we agree with DHS that its plan identifies activities (along with some performance measures and milestones) that will begin to address the challenges, this plan does not include specific initiatives that would ensure that the challenges are addressed in a prioritized and comprehensive manner. For example, the strategic plan for cybersecurity does not include initiatives to help stabilize and build authority for the organization. Further, the strategic plan does not identify the relative priority of its initiatives and does not consistently identify performance measures for completing its initiatives.

As DHS moves forward in identifying initiatives to address the underlying challenges it faces, it will be important to establish performance measures and milestones for fulfilling these initiatives.

DHS officials (as well as others who were quoted in our report) also provided detailed technical corrections, which we have incorporated in this report as appropriate.